(D)PoS 기반 블록체인의 거래 및 합의 방식 분석[1)]

한성호* 홍동연* 최낙준* 이나비* 김광조*

*카이스트 정보보호대학원

Analysis of Consensus and Transaction of (D)PoS-based Blockchains

Seongho Han* Dongyeon Hong* Nakjun Choi* Nabi Lee* Kwangjo Kim*

*Graduate School of Information Security, KAIST.

요 약

블록체인은 데이터 위조 방지와 데이터의 분산 저장을 제공하는 분산원장 기술이다. 블록체인에서 각 노드는 데이터가 기록된 블록을 분산 저장한다. 하지만 데이터를 분산 저장할 경우 동일한 데이터베이스를 유지하지 못하는 문제가 발생한다. 여러 노드에 동일한 데이터를 분산저장하기 위해 고안된 방식이 합의 알고리즘이다. 최초의 암호화폐인 비트코인은 PoW를 합의 알고리즘으로 채택하였다. 그러나 PoW 알고리즘은 불필요한 자원과 에너지가 소모된다는 단점을 가지고 있다. 이 문제를 해결하기 위해 등장한 합의 알고리즘이 PoS이다. 그리고 PoS에 위임의 형식을 추가한 것이 DPoS이다. 본 논문에서는 (D)PoS를 채택한 대표적인 블록체인 어플리케이션인 QTUM, ADA, EOS, LISK의 합의 알고리즘을 분석한다. 또한 각 코인의 블록 구조 및 거래 방식을 분석한다. 본 논문의 분석 결과를 추후 각 블록체인의 신뢰성 검증에 활용할 수 있는 가능성을 제시한다.

I. 서론

암호화폐와 기반 기술인 블록체인에 대한 관심이 높아지고 있다. 블록체인은 데이터 위조 방지와 데이터의 분산 저장을 제공하는 분산원장 기술이다. 블록체인에서 각 노드는 데이터가 기록된 블록을 저장한다. 하지만 데이터를 분산 저장할 경우 동일한 데이터베이스를 유지하지 못하는 문제가 발생한다. 여러 노드에 동일한 데이터를 분산저장하기 위해 고안된 방식이 합의 알고리즘이다.

최초의 암호화폐인 비트코인[1]은 작업 증명 방식(Proof of Work, PoW)을 합의 알고리즘으로 채택하였다. 그러나 PoW 알고리즘은 불필요한 자원과 에너지가 소모된다는 단점을 가지고 있다. 이 문제를 해결하기 위해 등장한 합의 알고리즘이 지분 증명 방식(Proof of Stake, PoS)[5]이다. 그리고 PoS에 위임의 형식을 추가한 것이 위임 지분 증명 방식[4](Delegated Proof of Stake, DPoS)이다.

본 논문에서는 (D)PoS방식에 대하여 설명하고, (D)PoS를 합의 프로토콜로 채택한 대표적인 블록체인 어플리케이션인 QTUM[2,9], ADA[11], EOS[7], LISK[8]의 합의 알고리즘을 분석한다. 세부적으로 각 코인을 블록 구조 및 거래 방식의 관점에서 분석한다.

1.1 논문의 구성

본 논문의 구성으로 Ⅱ장에서는 각 코인과 PoS 및 DPoS에 대하여 간략히 설명하고, Ⅲ장은 각 코인의 합의 알고리즘을 분석한다. Ⅳ장에서는 각 코인의 블록 구조 및 거래 방식을 분석한다. 마지막으로 Ⅴ장에서는 결론과 본 논

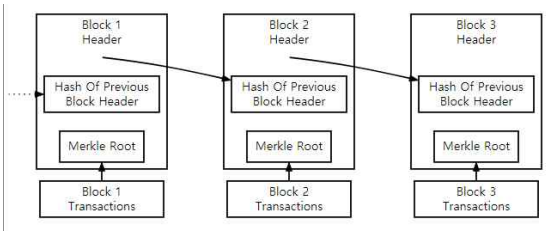
1) 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다. (No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)

문 성과를 이용한 추후 연구에 대한 가능성을 제시한다.

II. 배경지식

2.1 블록체인 어플리케이션

이 절에서는 QTUM, ADA, EOS, LISK에 대해 설명한다. [그림 1]은 블록체인의 기본적인 구조를 나타낸다.



[그림 1] 블록체인의 구조

QTUM[2,9] QTUM은 비트코인과 이더리움[6]을 합친 암호화폐로 볼 수 있다. 비트코인은 Unspent Transaction Output(이하 UTXO)을 기반으로 state를 관리하는 반면 이더리움은 Account를 기반으로 state를 관리한다. 두 암호화폐는 서로 호환이 되지 않는 구조이기 때문에 QTUM은 Account Abstraction Layer(이하 AAL)을 통해 둘 사이에 연결 다리를 놓았다. QTUM의 목표는 최초의 UTXO 기반의 스마트 컨트랙트 시스템을 구현하는 것이다.

ADA[11] ADA는 모바일에 최적화된 플랫폼인 Cardano를 통해 만들어진 암호화폐이다. 2015년에 IOHK에 설계됐고 2017년 10월에 공식 발표됐다. ADA는 DPoS를 채택한 암호화폐 중 하나이며 Ouroboros 프로토콜을 적용하면서 신뢰성이 상승하고 화폐의 가치가 증가했다.

EOS[7] EOS는 분산화된 어플리케이션의 확장성을 위해 고안된 블록체인 플랫폼 혹은 운영체제로 볼 수 있다. 계정, 인증, 데이터베이스, CPU 스케줄링 등 많은 기능들을 제공한다. 거래 처리량을 초당 백만 개로 유지하여 기존 암호화폐의 단점을 개선하는 것과 무료로 사용하는 것 등을 목표로 하고 있다.

LISK[8] LISK는 이더리움[6]처럼 블록체인 어플리케이션의 플랫폼을 제공하는 걸 목표로 한다. 이더리움과의 차이는 자바 스크립트를 기반으로 블록체인 어플리케이션의 플랫폼을 제공한다는 점이다. 다른 플랫폼들과 달리 개발자들은 메인 체인에 저장할 필요 없이 사이드 체인에 저장할 수 있다. 따라서 개발자들은 자신들의 체인을 구성하고 관리할 수 있다.

2.2 합의 알고리즘

지분 증명 방식(PoS)[5] 현재 가장 많이 사용되는 합의 알고리즘은 PoW이다. 하지만 PoW는 자원과 에너지가 과도하게 소모된다는 단점을 갖고 있다. 이를 대체하는 방법으로 PoS가 고안되었다. PoS는 PoW와 달리 채굴자가 없고 검증자가 존재한다. 검증자 선발 과정은 두 단계로 나뉜다. 우선 참가자들은 시스템을 통해 보증금을 예치한다. 이후 특정 규칙에 따라 최종적으로 검증자를 선발한다. 검증자가 된 사람은 거래의 유효성을 확인하고 블록을 생성한다. 검증자로 있는 기간이 길어질수록 받는 인센티브가 증가한다. 검증자는 유효하지 않은 거래를 거짓으로 유효하다고 할 수 없다.

위임 지분 증명 방식(DPoS)[4] DPoS는 PoS와 달리 누구에게나 검증자가 될 기회가 주어지지 않는다. 검증자가 되기 위해선 투표를 거쳐야 한다. 이때 명칭이 바뀌는데 투표를 통해 선출된 검증자를 대표자라고 한다. 선출된 대표자들은 블록을 생성한다. 블록을 확정하기 위해선 2/3 이상의 승인이 필요하다. 대표자의 지위는 일정 시간 이내에 블록 생성에 참여해야 유지된다. PoS와 달리 같은 시간에 훨씬 더 많은 거래를 처리할 수 있다는 점과 수수료가 없다는 장점이 있다.

III. 각 코인의 (D)PoS 합의 알고리즘 분석

QTUM PoS 2.0[9]에서 새 블록의 생성은 다음 조건을 충족해야 한다.

$$ProofHash < coins \times age \times target$$

ProofHash는 계산할 때 사용되지 않은 출력과 현재 시간을 고려하게 된다. 그러나 이 경우

double spending attack, coin age attack 등에 취약하기 때문에 QTUM은 최신 QTUM 코어에 PoS 3.0[10]을 채택하여 age를 제거하였다.

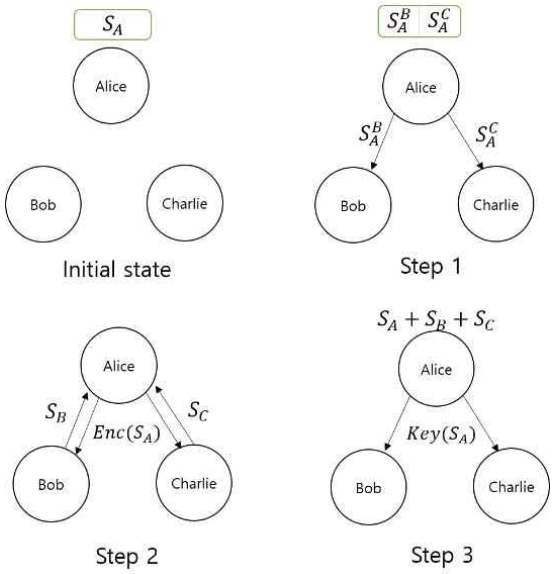
$$ProofHash < coins \times target$$

QTUM에서 블록 생성 권한은 지분 소유자가 보유한 코인의 양에 따라 결정된다. 지분 소유자들은 고정된 입력에 대해 그들이 제어하는 UTXO마다 하나의 해시를 수행하여 결과가 가중된 임계값 이하인지 여부를 확인한다. 해시되는 UTXO가 보유한 양이 많을수록 임계값에 가중치가 적용되므로 UTXO가 보유한 양이 많으면 더 높은 확률로 승리 할 수 있다. 조건을 충족시키는 해시가 생성되면 사용자는 블록을 전파한다. 그렇지 않다면 해시를 중지하고 다음 번 재생까지 기다린다.

16초마다 고정 입력 값이 변경되므로 지분 보유자들은 UTXO에 대한 새로운 해시 값을 생성하고 승자인지 확인할 수 있는 기회가 생긴다. 이것은 매 16초마다 추첨을 하는 것과 유사하다. UTXO에 의해 계산된 해시는 가중치가 있는 티켓을 나타낸다. 이 때 티켓에 가중치를 부여하는 것은 높은 가치의 UTXO를 여러 개의 작은 값으로 나눈 사용자가 더 많은 티켓을 얻지만 우승 확률은 증가하지 않도록 하기 위함이다. 난이도는 당첨된 티켓이 평균적으로 128초당 한 번만 발견되도록 설정된다.

ADA ADA는 DPoS 합의 알고리즘을 채택하였다. Ouroboros[3]를 이용하여 블록을 생성한다.

- Ouroboros: Ouroboros는 기존 PoS 합의 알고리즘의 문제를 해결하도록 설계되었다. 특히 Stake-Grinding Attack에 대응하는 것이 주요 목표이다. 현재 대부분의 PoS 프로토콜은 마지막 블록의 정보를 기반으로 무작위 변수를 계산한다. 그러나 마지막 블록 작성자는 사용자에게 유리한 랜덤 변수를 얻을 때까지 의도적으로 전송 세부 정보를 삭제하거나 포함할 수 있다. 따라서 Ouroboros는 Coin Tossing Protocol을 통해 위 문제를 해결하였다. Coin Tossing Protocol의 진행 과정은 [그림 2]와 같다.



[그림 2] Coin Tossing Protocol의 단계

[초기 상태] Alice, Bob 및 Charlie가 각각 랜덤 변수를 만든다.

[단계 1] 참가자들은 참가자 수만큼 랜덤 변수를 잘라서 모두에게 보낸다.

[단계 2] 각 랜덤 변수를 암호화하여 다른 참가자에게 보내면 받는 사람은 원래 랜덤 변수를 반환한다.

[단계 3] 다른 참가자의 랜덤 변수를 수신하자마자 수신자는 암호화 된 변수를 해독하기 위한 키를 보낸다. 키를 받은 참가자가 받은 키를 통해 암호를 해독하면 모든 사람이 랜덤 변수를 공유하게 된다.

위의 프로토콜을 사용하면 무작위로 분산된 변수 조각을 수집하고 복원할 수 있기 때문에 랜덤 변수를 안전하게 생성할 수 있다. 기존의 PoS 합의 알고리즘은 블록체인 참가자의 정보를 알 수 있는 경우에만 참여할 수 있는 보안상의 단점이 있었다. Ouroboros Genesis 프로토콜은 이를 해결하여 PoW와 유사한 수준의 보안을 제공할 것으로 예상되고 있다.

EOS EOS는 DPoS 합의 알고리즘을 사용한다. EOS는 지속적인 승인 투표 시스템을 통해 대표자라고 불리는 블록 생산자를 선택한다. 누구나 블록 생산에 참여할 수 있으며 일정 수준

의 토큰을 얻을 경우 대표자가 될 수 있다. EOS는 블록을 생성하고 네트워크에 영향력을 행사하는 21명의 대표단을 임명한다.

126라운드 동안 블록들이 생성된다. 21명의 대표는 6개의 블록을 각각 생성한다. 각 라운드가 시작할 때 토큰 소지자가 투표한 결과에 따라 21명의 고유한 대표자가 선정된다. 대표자는 15명 이상의 대표자가 합의한 순서대로 계획을 수행한다. 블록은 정확히 0.5초마다 생성되며 어느 시점이든 정확히 한 명의 대표자만 블록을 생성 할 권한이 있다. 블록이 예정된 시간에 생성되지 않으면, 그 시간 슬롯에 대한 블록은 생략된다. 하나 이상의 블록을 건너 뛸 때 블록체인에 0.5 초 이상의 간격이 존재한다.

대표자가 블록을 놓치고 24시간 내에 블록을 생성하지 않을 경우 블록 생성을 다시 시작할 의사가 있음을 알릴 때까지 대표자 목록에서 제거된다. 이를 통해 누락되는 블록을 최소화하여 네트워크를 원활하게 작동시킬 수 있다.

EOS는 대표자들이 정상적인 조건 하에서 블록을 생산하기 위해 협력하기 때문에 어떤 포크도 일어나지 않는다. 포크가 발생하면 합의는 자동으로 가장 긴 체인으로 전환된다. 이 방법은 블록이 블록체인 포크에 추가되는 비율이 동일한 합의를 공유하는 대표자의 비율과 직접적으로 연관되기 때문에 가능하다.

이에 더해 대표자는 동시에 2개의 포크에 블록을 생산할 수 없다. 대표자는 이중지불을 하면 지위가 박탈된다. 이중지불에 대한 암호학적 증거는 악용하는 사람을 자동으로 제거하는 데 사용할 수 있다.

LISK LISK 또한 DPoS를 사용한다. 블록을 생성하는 대표자 N명(현재 N=101)은 모든 참여자에 의해 선출된다. 모든 참여자는 대표자가 될 수 있지만 필요한 지분을 보유한 참여자만 블록을 생성 할 수 있다. 각 참여자는 최대 101명까지 투표 할 수 있으며 표의 영향력은 참여자가 소유하는 토큰 양에 따라 달라진다.

시스템 내에서 한 라운드는 대표자 수와 동일한 N블록으로 구성된다. 각 라운드의 시작 부분에서 각 대표는 블록 생성 프로세스에서 그들의 위치를 나타내는 슬롯에 지정되어 있다. 각 대표는 한 라운드 동안 정확히 하나의 블록을 생성한다. 블록은 10초마다 생성된다. 각 블록에는 25개의 거래 내역이 포함된다. 각 블록은 서명 된 후 대표자에 의해 네트워크로 전파된다. 블록이 네트워크에 도달하면 다음 대표자가 할당된 슬롯에서 블록을 생성한다. 선출 된 대표자가 라운드 도중 블록을 생산할 수 없다면, 다른 대표자가 블록을 대신 생성한다.

블록 생성을 위해서 51%의 동료가 broadhash 합의를 유지해야한다. 포크를 막기 위해서 broadhash 합의가 필요하다. Broadhash는 데이터베이스에 있는 지난 5개 블록에 집계된 롤링 해시로 설정된다. 동일한 블록을 가진 모든 노드는 시스템 헤더를 통해 동일한 정보를 생성하고 해당 정보를 전파한다. 이를 통해 유효한 노드 중 대다수가 블록을 생산하는 것에 동의하게 된다.

IV. 각 코인의 블록 구조 및 거래 방식 분석

QTUM

- 블록구조: 비트코인의 UTXO 모델을 기반으로 하기 때문에 비트코인 블록구조[그림 3]와 유사하다.

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

[그림 3] 비트코인의 블록 구조

- 거래 방식: 거래의 전체적인 흐름은 비트코인과 유사하다고 볼 수 있다. 그러나 OP_EXEC, OP_EXEC_ASSIGN, OP_TXHASH 3가지의 명령어의 추가로 차이가 발생한다. 3가지의 명령어는 비트코인의 명령어와 이더리움의 명령어를 이어주는 매개체로 볼 수 있는데 AAL과 연관이 있다. 채굴 과정에서 거래를 추가할 때 EXEC의 유무에 따라 절차가 달라진다. EXEC이 있으면 수수료를 계산하는 작업을 한 후 bytecode를 실행시켜 특정 프로세스를 실행한다. 이후 블록을 생성하고 연결하는 작업에서 같은 EXEC의 bytecode를 실행하고 생성된 거래를 queue에 추가한다. 그리고 TXHASH 명령어를 통해 검증 작업을 거친다. 거래가 유효하다면 블록을 승인한다.

ADA

- 블록구조: 메인 블록과 제네시스 블록으로 나뉜다. 각 블록은 헤더와 바디로 구분된다. 헤더에는 4가지의 항목이 있다. 이전 블록의 서명, 바디의 증명, 합의 알고리즘에 필요한 데이터와 그 외 데이터로 나뉜다. 바디 부분에는 총 4가지의 페이로드가 있는데, transaction, SSC(Shared Seed Computation), delegation와 update가 있다. 제네시스 블록에는 3가지의 정보가 더 존재한다. 현재 epoch의 index와 slot leader의 리스트, 체인을 연결하기 위한 난이도이다.

- 거래 방식: 거래 내역은 자금 전송 시점에 생성된다. 거래의 전체적인 흐름은 다음과 같다. (1) 거래를 만들고 개인 비밀키로 서명한다. (2) 자신의 주변에 거래를 전송한다. (3) Slot leader가 검증한 이후 로컬 데이터에 저장한다.

거래는 간단히 input과 output data로 나뉜다. Input은 현재 거래의 ID와 대응되는 output의 index 정보와 금액을 갖고 있다. Output은 받는 노드의 주소와 금액 정보를 갖고 있다. 돈을 전송할 때 거래에 있던 output이 다른 거래의 input으로 들어간다. 이때 UTXO(Unspent Transaction Output)라는 개념이 필요하다. A의 주소로 향하는 거래가 B의 주소로 간다고 가정하면, A의 주소를 가리키던 output이 거래의 input으로 들어가고 B의 주소를 가리키는 output이 된다. 이후 slot leader가 검증하면 거래가 성립된다.

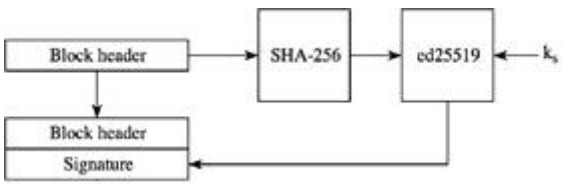
EOS

- 블록구조: EOS의 거래 방식은 Steem, BitShare와 유사하다. 따라서 EOS의 블록구조는 BitShare의 블록구조와 유사할 것으로 추정된다. BitShare의 블록은 헤더와 바디로 구성된다. 헤더 부분에는 이전 블록 ID, 블록 번호, 타임스탬프, transaction 요약, 다음 비밀 해쉬, 이전 비밀이 포함된다. 바디에는 블록 ID, 공개키, 헤더 서명, 블록 크기, 서명된 거래들이 포함된다. 데이터와 코드가 분리되어있어 계약에서 병목 현상을 해결할 수 있는 것이 특징이다.

- 거래 방식: 거래 방식은 총 3가지 필드로 구성된다. 범위(Scope), 메시지(Message), 스케쥴링이다. Scope는 읽히거나 쓰여질 데이터의 범위를 구체화한다. 만약 메시지가 범위 밖에 있는 데이터를 읽거나 쓰려고 시도하면 거래는 실패한다. Message는 코드, 타입, 수신자, 권한, 데이터 정보를 포함한다. EOS에서는 권한이 명시적으로 정의되므로 필요한 서명 전부를 자동으로 확인한다. 스케쥴링은 블록을 병렬적으로 실행할 수 있는 기회를 제공한다.

LISK

- 블록구조: LISK의 블록 헤더는 블록 버전, 타임스탬프, 이전 블록 ID, 거래량, 전송된 총 LISK 양, 총 수수료 금액, 대표자에 대한 보상, 페이로드 길이, 페이로드 해시값, 대표자의 공개키로 구성된다. 블록 헤더는 서명이 필요하다. 서명 과정은 [그림 4]와 같다. 블록 헤더의 SHA-256 해시를 생성하고 대표자의 키 암호를 사용하여 서명한다.



[그림 4] 블록헤더의 서명 과정

- 거래 방식: LISK에서 주로 사용되는 거래 유형은 총 5가지가 있다. 지정된 LISK 주소로 자금 전송, 두 번째 암호 등록, 대표자 등록, 대표자를 위한 투표 등록, 다중 서명 등록 유형이다. 유형에 관계없이 모든 거래는 네트워크에서 승인되기 전에 발신자가 서명해야한다. 거래에 서명하는 과정은 모든 거래에서 동일하며 블록 헤더의 서명 과정과도 동일하다. 단 데이터 블록에 포함 된 추가 정보는 거래 유형에 따라 다르다.

모든 거래는 3가지 단계로 구성된다. (1) 거래에 필요한 필드 지정 후 거래 객체를 작성한다. (2) 객체에 서명한다. (3) 거래 수수료를 계산한다.

자금을 전송하는 유형의 경우에는 대표자가 해당 거래를 처리하는 과정이 추가된다.

V. 결론

본 논문에서는 PoS방식과 DPoS방식에 대하여 설명하고, (D)PoS를 합의 프로토콜로 채택한 대표적인 블록체인 어플리케이션인 QTUM, ADA, EOS, LISK의 합의 알고리즘을 분석하였다. 세부적으로 각 코인을 블록 구조 및 거래 방식의 관점에서 분석했다. 이를 통해 (D)PoS 방식이 가질 수 있는 한계를 발견하고 개선 방안을 탐구할 수 있다. 향후 연구로 (D)PoS의 단점을 개선한 합의 알고리즘을 제안할 수 있을 것이다.

한편 블록체인의 신뢰성 검토에 본 논문을 활용할 수 있다. 블록체인의 합의 알고리즘은 이중지불을 방지하므로 블록체인의 신뢰도와 직결되어있다. 따라서 블록체인에 한층 더 높은 신뢰성을 제공하기 위한 연구에 활용할 수 있다.

[참고문헌]

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system” 2008.

[2] P. Dai, N. Mahi, J. Earls, A. Norta, “Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform”

[3] Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol" Annual International Cryptology Conference. Springer, Cham, 2017.

[4] Larimer, Daniel. "Delegated proof-of-stake (dpos)" Bitshare whitepaper, 2014.

[5] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake" self-published paper, 2012.

[6] https://github.com/ethereum/wiki/wiki/White-Paper

[7] https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[8] https://lisk.io/documentation

[9] https://qtum.org/en/

[10] https://blackcoin.co/

[11] https://whycardano.com/